QUADRIFOR
ISTITUTO BILATERALE PER LO SVILUPPO
DELLA FORMAZIONE DEI QUADRI DEL TERZIARIO

Policy sulla sicurezza delle informazioni

Rev. 1.0

QUADRIFOR
ISTITUTO BILATERALE PER LO SVILUPPO
DELLA FORMAZIONE DEI QUADRI DEL TERZIARIO

Sommario

1. Introduzione

1.1 Finalità

La presente policy regola gli accorgimenti di sicurezza adottati da Quadrifor per proteggere l'integrità, la riservatezza e la disponibilità dei dati personali, nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 (d'ora in poi GDPR, General Data Protection Regulation) in particolare all'art. 32.

1.2 Ambito di applicazione e definizioni

La presente Procedura si applica ad ogni *Utente* e per ogni sede aziendale.
Per *Utente* si intende, pertanto, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), consulente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.
Per *Istituto* si intende, invece, l'Istituto Quadrifor, titolare dei beni e delle risorse informatiche ivi disciplinate, la quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

1.3 Responsabilità personale dell'utente

Ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Istituto, è tenuto al rispetto di questa policy ed è personalmente responsabile del suo mancato rispetto in caso di negligenza o dolo.

2. Organizzazione della Sicurezza delle Informazioni

Quadrifor ha una funzione di protezione dei dati personali (DPO) che è stata ratificata ed è supportato dal management aziendale. Quadrifor si assicura di diffondere tra il suo personale la cultura della sicurezza delle informazioni.

Le misure adottate comprendono:

a) Identificazione e ingaggio di un responsabile della protezione dei dati (RPD) o DPO (Data Protection Officer).
b) Il DPO Quadrifor riporta direttamente al Titolare o al Responsabile del trattamento Quadrifor ed è indipendente per quanto attiene alla gestione operativa dei suoi compiti.
c) Quadrifor ha un insieme completo di politiche di sicurezza delle informazioni, approvate dal Top Management e diffusi a tutto il personale.

d) Le politiche di sicurezza Quadrifor sono riviste almeno annualmente e aggiornate in caso di necessità.
e) Tutto il Personale Quadrifor ha firmato accordi di riservatezza che si applicano durante e successivamente al rapporto di lavoro.
f) La superficialità o l'intenzionalità del personale nel seguire le politiche di sicurezza delle informazioni può essere trattata come una questione disciplinare e portare a sanzioni.
g) A tutto il Personale Quadrifor è stata data formazione dei fondamentali di sicurezza delle informazioni e della privacy.
h) Quadrifor si impegna per il miglioramento continuo della propria sicurezza.

3. Sistema di Gestione della Sicurezza delle Informazioni

Quadrifor ha in atto una procedura di valutazione d'impatto sulla protezione dei dati (DPIA) per valutare i rischi per la sicurezza dei dati personali, per gestirne il trattamento e la mitigazione e migliorare costantemente la sicurezza delle informazioni.

Ulteriori dettagli sono disponibili nella procedura DPIA (Data Protection Impact Assessment)

4. Accesso fisico

L'accesso fisico ai dati personali è protetto.

Misure adottate:

a) Quadrifor gestisce il sito WEB www.quadrifor.it così come tutto il parco applicativo mediante una società specializzata. I dati gestiti da terzi sono in un data center italiano con un perimetro fisico delimitato e protetto, rigorosi controlli fisici di controllo accesso, sorveglianza 24x7x365. Solo personale autorizzato ha accesso ai locali del centro dati.
b) Il cablaggio fisico che trasporta dati personali o in ogni caso relativi al sistema informativo è schermato e protetto da interferenze e danni.
c) Il data center di esercizio è fisicamente protetto contro le calamità naturali, attacchi dannosi e incidenti.
d) Il data center di esercizio è protetto da interruzioni di corrente ed altre interruzioni causate da guasti nei servizi di supporto, ed è mantenuto correttamente.
e) Apparecchiature o supporti di memoria contenenti dati personali (compresi i casi di difettosità o di dismissione) vengono cancellati in modo sicuro prima della rimozione e l'affidamento allo smaltimento rifiuti.
f) Quando i dati personali vengono copiati elettronicamente da Quadrifor all'esterno del data center di produzione, viene mantenuto un adeguato livello di sicurezza fisica e, in ogni caso, i dati vengono cifrati.

5. Sistema di accesso

I sistemi di elaborazione dati Quadrifor vengono utilizzati solo da utenti autorizzati e autenticati sulla rete aziendale.

Misure adottate:

a) L'accesso ai sistemi interni Quadrifor è concesso solo a la personale Quadrifor e/o ai dipendenti autorizzati dei subappaltatori con modalità di accesso strettamente limitato alla funzione assegnata.
b) Tutti gli utenti accedono ai sistemi Quadrifor con un identificatore univoco (ID utente) e una password.
c) Quadrifor ha stabilito una politica delle password che ne vieta la condivisione e che richiede la modifica ad intervalli periodici nonché impedisce la permanenza di password di default.
d) Tutte le password devono soddisfare i requisiti minimi definiti e sono memorizzati in forma criptata. Ogni computer ha uno screensaver protetto da password.
e) E' necessario una secondo livello di autenticazione per l'accesso ai sistemi online contenenti dati personali.
f) Quadrifor ha una procedura per disattivare gli utenti e il loro accesso quando un dipendente lascia l'azienda.
g) Un sistema di Intrusion Detection (IDS) o Intrusion Prevention System (IPS) viene utilizzato presso il Data Center per identificare e prevenire potenziali accessi non autorizzati.

6. Accesso ai dati

Le persone incaricate di effettuare trattamento di dati personali hanno accesso solo ai dati per i quali sono autorizzati.

Misure adottate:

a) Limitazione dell'accesso del personale ai dati a ai sistemi informativi in base alla stretta necessità in virtù delle proprie funzioni operative.
b) La formazione del personale comprende i diritti di accesso e gli orientamenti generali sulla definizione e l'uso dei dati personali.
c) Se del caso, Quadrifor impiega tecniche di minimizzazione e di pseudonimizzazione dei dati personali per ridurre la probabilità di accessi non autorizzati.
d) L'ambiente di produzione per il sito web così come per tutte le applicazioni Quadrifor è separata dall'ambiente di sviluppo e test, e il personale esterno che effettua sviluppo non ha accesso all'ambiente di produzione.

e) Quadrifor utilizza software anti-malware aggiornati su tutti i computer e i server identificati come appropriati.
f) Quadrifor utilizza firewall adeguatamente configurati per i servizi del sito WEB.
g) Quadrifor si assicura che l'azienda che gestisce in outsourcing il sistema informativo, abbia posto gli amministratori in condizione di ricevere avvisi e notifiche dai fornitori di software di sistema e altre fonti di avvisi di sicurezza e installi regolarmente e in modo efficiente le patch software di sistema.

7. La trasmissione dei dati

Quadrifor impedisce che i dati personali possano essere letti, copiati, modificati o cancellati da persone non autorizzate durante le trasmissioni.

Misure adottate:

a) L'accesso degli utenti ai servizi WEB Quadrifor è protetto da SSL.
b) Impiego di crittografia forte per tutte le altre trasmissioni di dati personali al di fuori del data center.
c) Tutti i dati personali memorizzati al di fuori del data center sono protetti da crittografia forte.

Il Cliente è responsabile per la sicurezza dei dati personali una volta che questi gli siano stati trasmessi da Quadrifor al Cliente, compresa la circostanza in cui i suddetti dati siano scaricati dagli utenti dei Clienti.

8. Riservatezza e integrità dei dati personali

I Dati Personali rimangono confidenziali, intatti, completi e aggiornati durante il trattamento.

Misure adottate:

a) Quadrifor chiede formalmente la sua società di gestione IT e sviluppo software (La gestione IT e lo sviluppo del software sono in outsourcing) di avere personale adeguatamente formato in tema di sicurezza delle informazioni.
b) Tutte le modifiche al software vengono effettuate attraverso un meccanismo di approvazione formale che tenga traccia delle richieste di modifica e delle relative approvazioni prima della realizzazione.
c) Tutti le funzioni di crittografia utilizzate all'interno delle applicazioni Quadrifor utilizzando gli standard del settore.

9. Disponibilità

I dati personali sono protetti dalla distruzione o perdita accidentale e vi è la possibilità del ripristino tempestivo della loro disponibilità in caso di incidente.

Misure adottate:

a) Quadrifor utilizza un elevato livello di ridondanza sui dati di produzione in modo che il guasto o la mancanza di disponibilità di un unico sistema o componente non influisca sulla disponibilità generale delle informazioni.
b) Il data center dispone di più fonti di alimentazione, generatori on-site con batterie di back-up per salvaguardare la disponibilità di alimentazione elettrica.
c) Il data center ha più punti di accesso a Internet per salvaguardare la connettività.
d) Il data center viene monitorato 24x7x365 per quanto attiene ad alimentazione elettrica, connettività e continuità dei sistemi.
e) Quadrifor, attraverso i suoi fornitori, utilizza sforzi ragionevoli per creare copie di back-up dei dati personali criptate e conservarli in una posizione geograficamente separata al data center.
f) Quadrifor, attraverso i suoi fornitori, esegue test di ripristino da tali backup con periodicità almeno trimestrale.

10. Controllo dei trattamenti

I dati personali trattati per conto di un utente vengo elaborati esclusivamente in conformità con le autorizzazioni e le istruzioni ricevute dal Cliente.

Misure adottate:

a) Quadrifor agisce come responsabile del trattamento dei dati personali e memorizza ed elabora i dati personali, al fine di effettuare i trattamenti sotto le istruzioni del utente e per le finalità da lui stabilite.
b) Quadrifor non accede ai Dati Personali degli utenti, eccezion fatta per le finalità necessarie per lo svolgimento del suo servizio, su richiesta del Titolare o dell'interessato, per ragioni di sicurezza o per ogni altro adempimento di legge.
c) Quadrifor impiega un numero limitato di fornitori, che incarica come responsabili del trattamento. Essi sono vincolati al rispetto della riservatezza dei Dati Personali e a seguire le sue procedure e policy di sicurezza delle informazioni. Un elenco è disponibile su richiesta.
d) Quadrifor ha adottato procedure e policy che la rendono compliant con il Regolamento Europeo 2016/679 (General Data Protection Regulation - GDPR)

11. Separazione dei dati

Dati personali raccolti per scopi diversi vengono trattati separatamente.

Misure adottate:

a) Quadrifor utilizza un'architettura multi-tenant per realizzare la separazione logica dei dati personali provenienti da più utenti.
b) I quadri e le aziende iscritte hanno accesso solo ai dati personali di propria competenza.

12. Gestione degli incidenti di privacy

In caso di violazione della sicurezza dei dati personali, l'effetto della violazione è ridotto al minimo. Le Autorità e/o gli interessati vengono informati secondo le prescrizioni del regolamento.

Esiste un'apposita procedura di Data Breach alla quale si rimanda per la descrizione delle azioni adottate.

Viene tenuto un apposito registro dei Data Breach, sul quale vengono annotati gli incidenti di privacy, anche quelli il cui esito non comporta, a norma di legge, la notifica al Garante e/o agli interessati.

13. Compliance

Quadrifor verifica continuamente l'efficacia di queste misure tecniche e organizzative.

Misure adottate:

a) Quadrifor conduce regolarmente verifiche interne ed esterne attraverso una procedura di periodica valutazione d'impatto sulla protezione dei dati (DPIA).
b) Quadrifor prende misure ragionevoli per assicurare che il personale sia a conoscenza e rispetti le misure tecniche e organizzative di cui al presente documento. In particolare il DPO fornisce la formazione necessaria e continui aggiornamenti in merito alla normativa e agli accorgimenti comportamentali in tema di data protection.
c) Quadrifor conduce test di vulnerabilità e di penetrabilità annuali sull'ambiente di produzione.

14. Documentazione di riferimento

ID	TITOLO	DATA EMISSIONE
1	Regolamento Europeo 2016/679 – General Data Protection (GDPR)	Ottobre 2016
2	Linee guida in materia di notifica delle violazioni di dati personali (Data Breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 Adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 Versione emendata e adottata il 6 febbraio 2018	Febbraio 2018
3	Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali http://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili	

15. Definizioni

TERMINE	DEFINIZIONE
Dato personale	Dato atto ad individuare univocamente una persona fisica
Dato sensibile - categorie particolari di dati personali	Nella pratica operativa si possono considerare le seguenti tipologie: o I dati idonei a rivelare le origini razziali ed etniche. o I dati idonei a rivelare le convinzioni religiose o filosofiche o l'appartenenza sindacale o I dati idonei a rivelare lo stato di salute o alla vita sessuale o I dati idonei a rivelare le convinzioni politiche o Dati di carattere giudiziario o Dati biometrici intesi a identificare in modo univoco una persona fisica

	○ Dati genetici

16. Approvazione della Policy

La presente Procedura è stata approvata dal Responsabile del trattamento dott. Roberto Savini Zangrandi in data 18/05/2018.

Si chiarisce che l'Istituto si riserva di effettuare eventuali variazioni al presente regolamento o al suo allegato, e che le stesse verranno comunicate agli Utenti.

Roma, 18 maggio 2018